

Claims

We claim:

1. A method of securely transmitting digital text comprising:
 - a) utilizing a biometric sensor to generate a key for a customer;
 - b) utilizing said key to encrypt said digital text;
 - c) transmitting said encrypted digital text to said customer; and
 - d) utilizing said biometric sensor to decrypt said encrypted digital text.
2. The method of claim 1 wherein said digital text comprises movies in a studio film archive.
3. The method of claim 1 wherein said digital text comprises songs in a music archive.
4. The method of claim 1 wherein said digital text comprises financial information in a finance archive.
5. The method of claim 1 wherein said digital text comprises personal medical information.
6. The method of claim 1 wherein said digital text comprises master tapes generated in a recording studio.
7. The method of claim 1 wherein said digital text comprises government information.
8. The method of claim 1 wherein said key contains no biometric information.
9. The method of claim 1 wherein said encryption step is performed seven times.
10. The method of claim 1 wherein said encryption step comprises decryption limitations.
11. The method of claim 10 wherein said decryption limitations comprise expiration time periods.
12. The method of claim 10 wherein said decryption limitations comprise a numeric limit to the number of times the text may be decrypted.
13. The method of claim 1 wherein said transmission step is performed electronically.

14. The method of claim 1 wherein said transmission step is performed physically.
 15. The method of claim 1 wherein transmission of said text to said customer does not contain said key.
16. A symmetric key system for securely transmitting digital text comprising:
- a) digital text;
 - b) a customer;
 - c) a key unique to said customer;
 - d) a biometric sensor;
- wherein said digital text is encrypted using said key prior to transmission,
wherein said encrypted digital text is transmitted without said key,
wherein said customer accesses said key using said biometric sensor,
wherein said customer decrypts said digital text utilizing said key.
17. The symmetric key system of claim 16 wherein said biometric sensor comprises a digital text reader, wherein said customer simultaneously accesses said key and decrypts said proprietary digital text using said biometric sensor/digital text reader.
18. The symmetric key system of claim 17 wherein said biometric sensor/digital text reader is portable.